Cloudera Runtime 7.0.2

Ranger Auditing

Date published: 2019-11-01
Date modified:

https://docs.cloudera.com/

Legal Notice

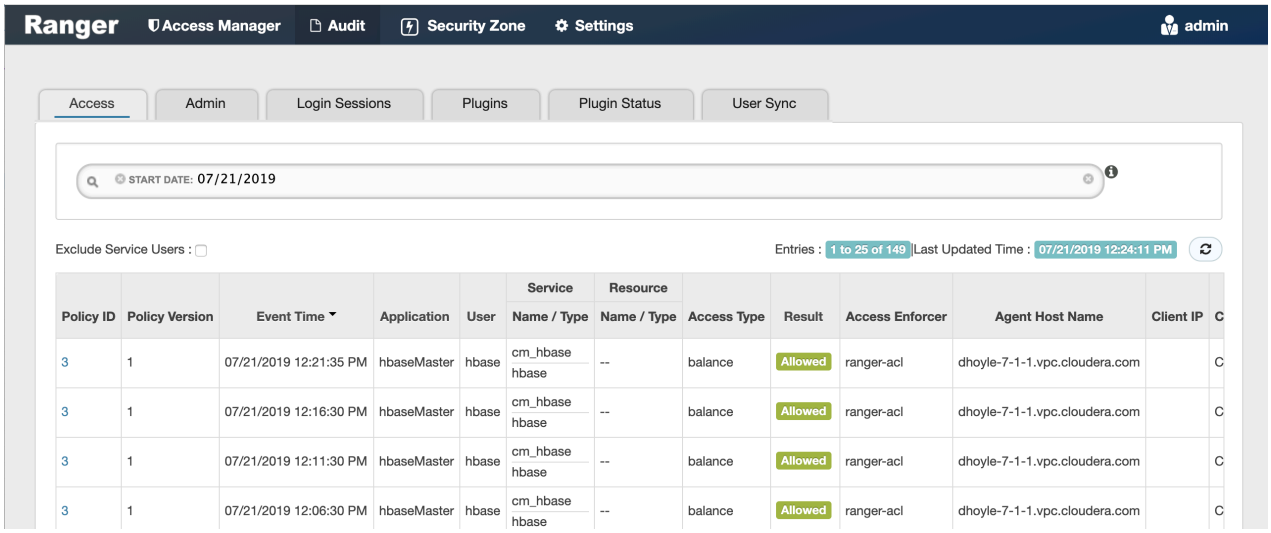
Contents

Audit Overview

Apache Ranger provides a centralized framework for collecting access audit history and reporting data, including filtering on various parameters. Ranger enhances audit information obtained from Hadoop components and provides insights through this centralized reporting capability.

Managing Auditing with Ranger

To explore options for auditing policies in Ranger, click Audit in the top menu.



There are six tabs on the Audit page:

- Access
- Admin
- Login sessions
- Plugins
- Plugin Status
- User Sync

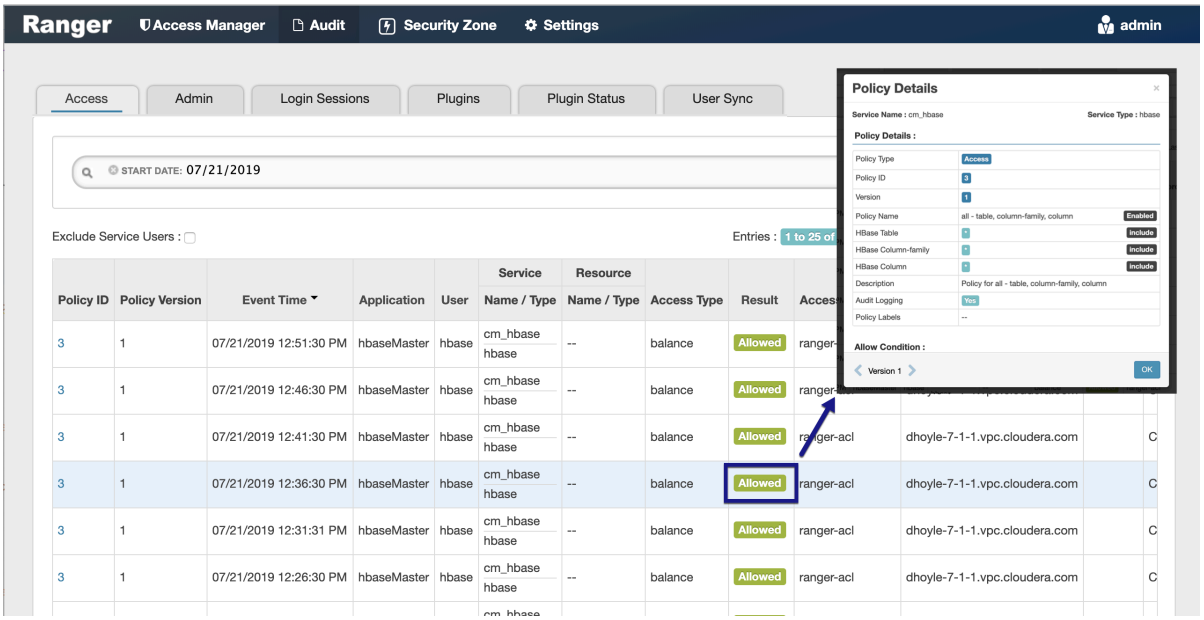
View audit details

How to view operation details in Ranger audits.

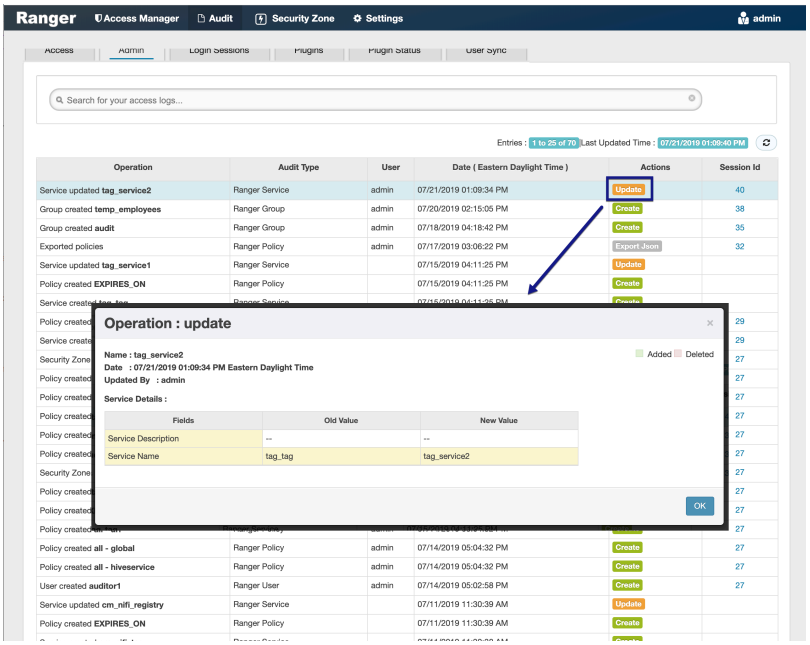
Procedure

To view details for a particular operation, click any tab, then Policy ID, Operation name, or Session ID.

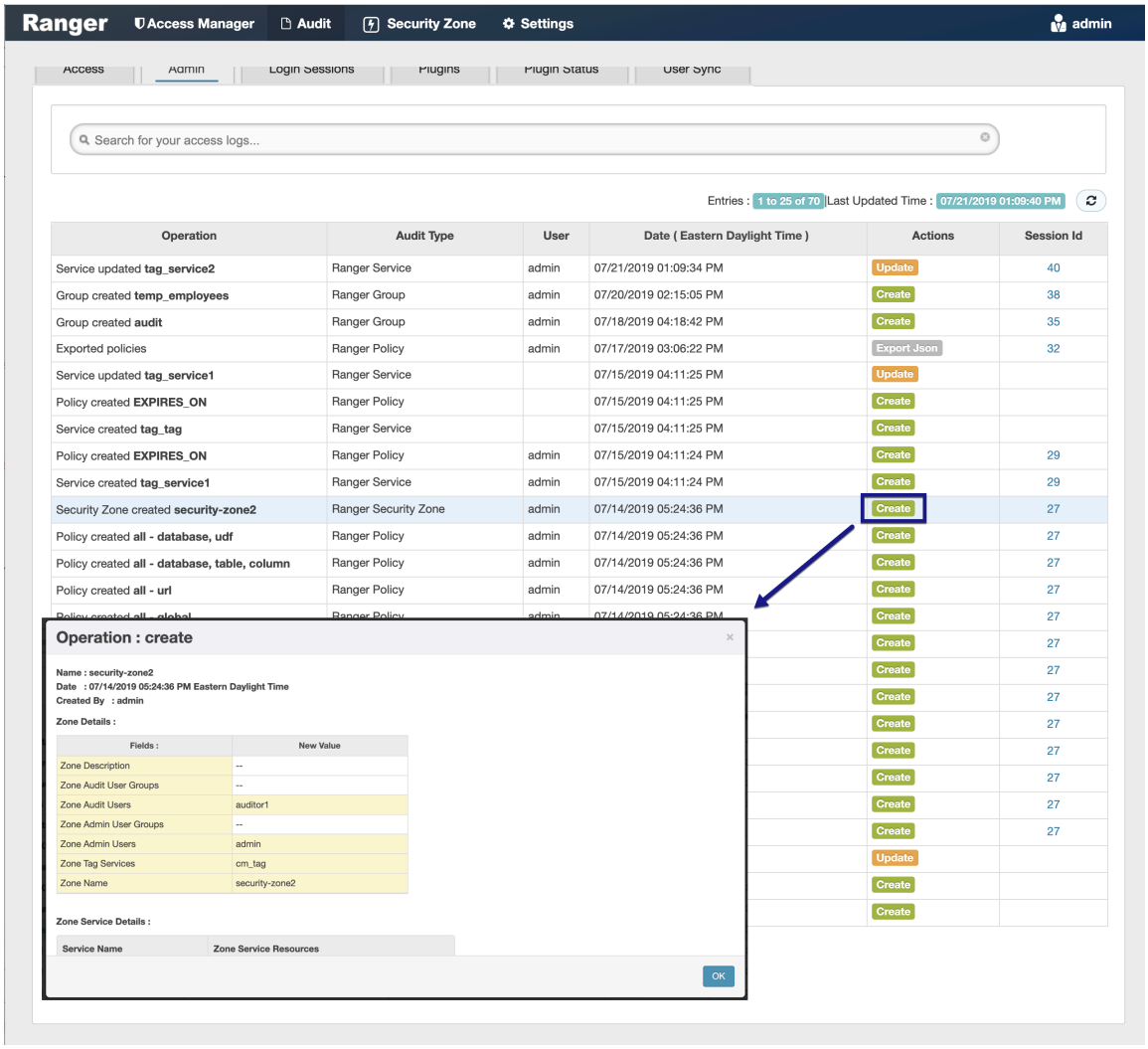
Audit > Access: HBase Table



Audit > Admin: Update

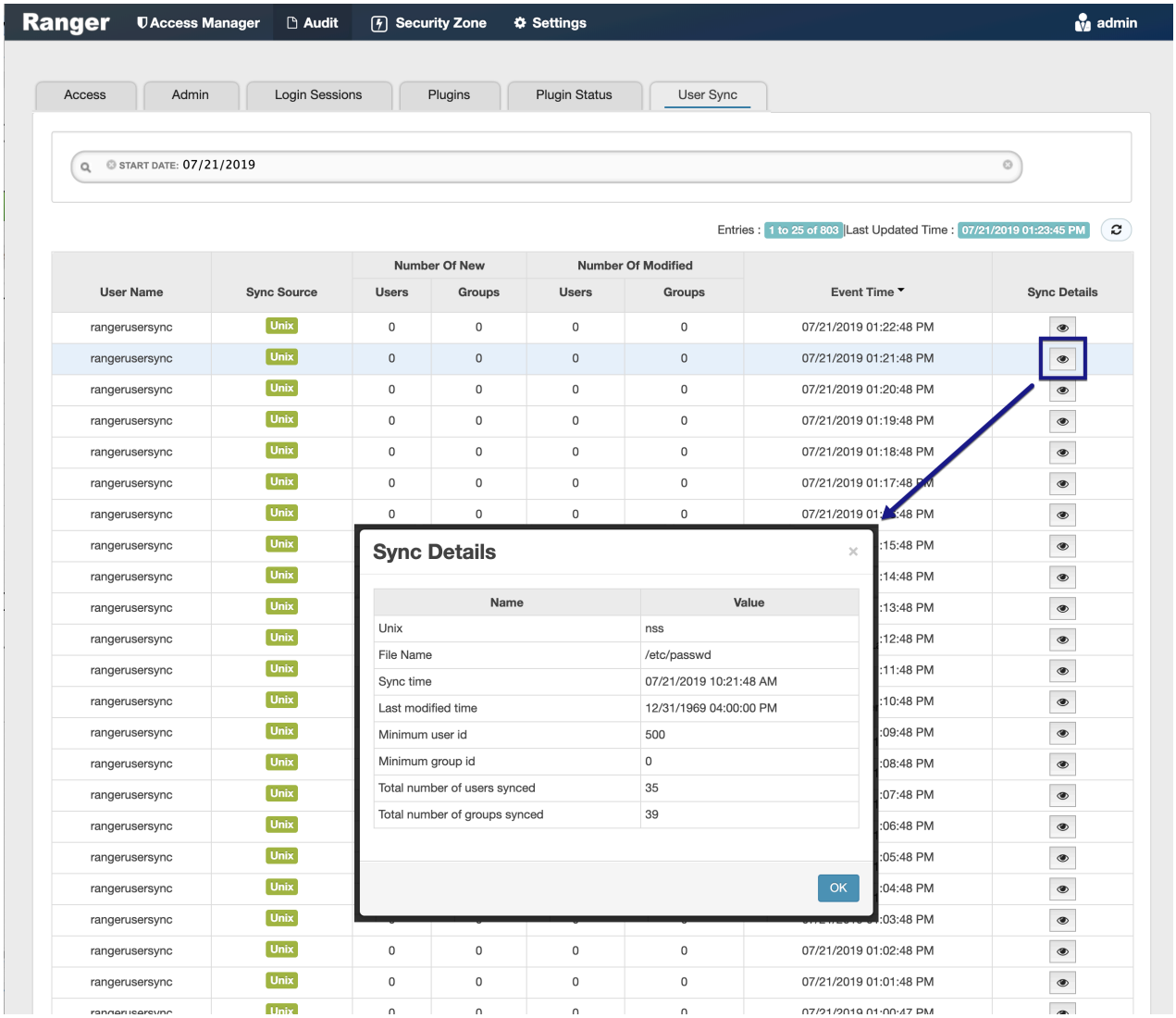


Audit > Admin: Create



Operation	Audit Type	User	Date (Eastern Daylight Time)	Actions	Session Id
Service updated **tag_service2**	Ranger Service	admin	07/21/2019 01:09:34 PM	Update	40
Group created **temp_employees**	Ranger Group	admin	07/20/2019 02:15:05 PM	Create	38
Group created **audit**	Ranger Group	admin	07/18/2019 04:18:42 PM	Create	35
Exported policies	Ranger Policy	admin	07/17/2019 03:06:22 PM	Export Json	32
Service updated **tag_service1**	Ranger Service		07/15/2019 04:11:25 PM	Update	
Policy created **EXPIRES_ON**	Ranger Policy		07/15/2019 04:11:25 PM	Create	
Service created **tag_tag**	Ranger Service		07/15/2019 04:11:25 PM	Create	
Policy created **EXPIRES_ON**	Ranger Policy	admin	07/15/2019 04:11:24 PM	Create	29
Service created **tag_service1**	Ranger Service	admin	07/15/2019 04:11:24 PM	Create	29
Security Zone created **security-zone2**	Ranger Security Zone	admin	07/14/2019 05:24:36 PM	Create	27
Policy created **all - database, udf**	Ranger Policy	admin	07/14/2019 05:24:36 PM	Create	27
Policy created **all - database, table, column**	Ranger Policy	admin	07/14/2019 05:24:36 PM	Create	27
Policy created **all - url**	Ranger Policy	admin	07/14/2019 05:24:36 PM	Create	27
Policy created **all - global**	Ranger Policy	admin	07/14/2019 05:24:36 PM	Create	27
				Create	27
				Create	27
				Create	27
				Create	27
				Create	27
				Create	27
				Create	27
				Create	27
				Update	
				Create	
				Create	

Audit > User Sync: Sync details



Create a read-only Admin user (Auditor)

Creating a read-only Admin user (Auditor) enables compliance activities because this user can monitor policies and audit events, but cannot make changes.

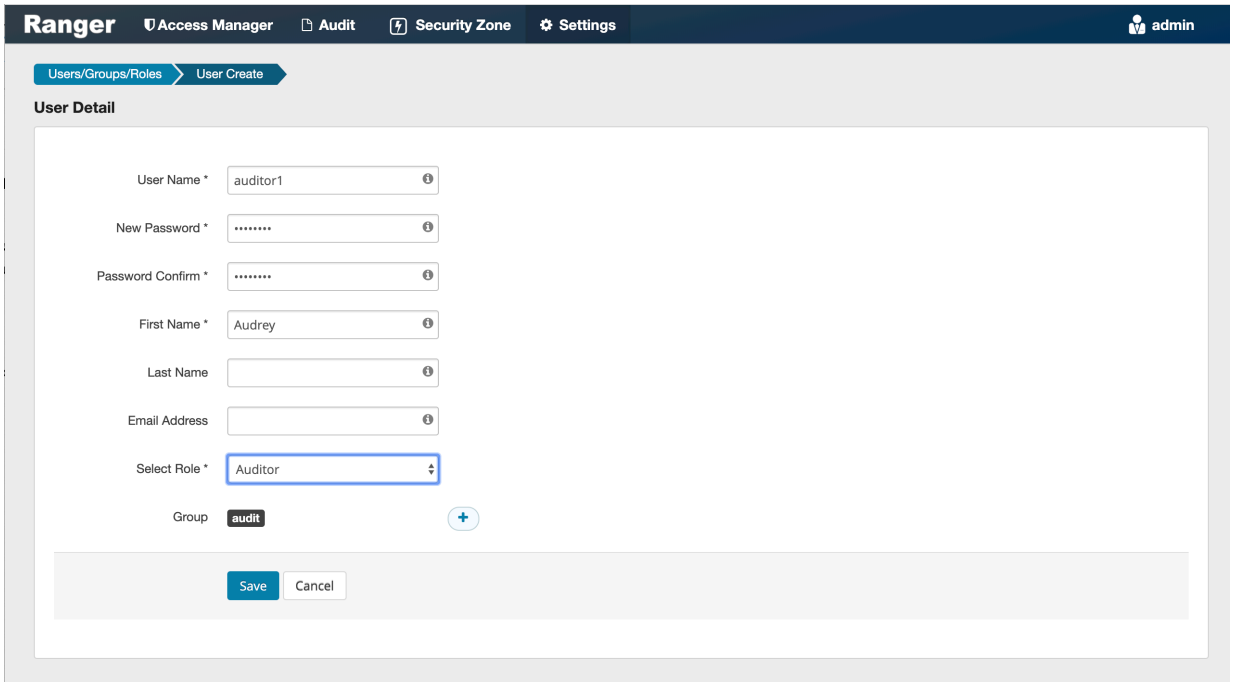
About this task

When a user with the Auditor role logs in, they see a read-only view of Ranger policies and audit events. An Auditor can search and filter on access audit events, and access and view all tabs under Audit to understand access events. They cannot edit users or groups, export/import policies, or make changes of any kind.

Procedure

1. Select Settings > Users/Groups/Roles.
2. Click Add New User.

3. Complete the **User Detail** section, selecting Auditor as the role:



4. Click Save.